Notice of Allowability	**Application No.** 09/942,176	**Applicant(s)** NESSETT, DANNY M.
	Examiner Thomas M. Ho	**Art Unit** 2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *11/01/05*.

2. ☒ The allowed claim(s) is/are *1-25*.

3. ☒ The drawings filed on *28 August 2001* are accepted by the Examiner.

4. □ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) □ All b) □ Some* c) □ None of the:
   1. □ Certified copies of the priority documents have been received.
   2. □ Certified copies of the priority documents have been received in Application No. _____ .
   3. □ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. □ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. □ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) □ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
   1) □ hereto or 2) □ to Paper No./Mail Date _____.
   (b) □ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. □ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. □ Notice of References Cited (PTO-892)
2. □ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. □ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. □ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. □ Notice of Informal Patent Application (PTO-152)
6. □ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. □ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. □ Other _____.

1. Claims 1-25 are pending.

Reasons for Allowance

2. Applicant's claims appear to recite an improvement or modification over a standard Otway-Rees encryption protocol. Applicant has corrected minor informalities, overcome and the Examiner has found A***pplicant's arguments regarding how the access point is involved such that processing to be shared to be persuasive. Accordingly the rejection of the claims under 35 USC 112 are withdrawn.***

Furthermore, in the action dated 1/5/05, the Examiner presented a rejection under 35 USC 103(a) over (Menezes et al., Handbook of Applied Cryptography) in view of (Schneier, Applied Cryptography) and Lincke et al., US patent 6253326.

In reference to claim 1:

(Menezes et al., , pgs. 503-504 Sections on Otway-Rees protocol, Handbook of Applied Cryptography) discloses in a network access point, a method of processing encrypted communication, according to an encryption/decryption process, said method comprising:

- Receiving a first message from a wireless client, said first message comprising first values for a first random number and information identifying said wireless client and said access point and a first message authentication code of said information in said first message signed using a first signing key,

  - where the first wireless client is Alice, the first random number is the Nonce A, information identifying the client is her name, information identifying the access point is Bob, the message authentication code is an index number, and the message is signed message is the encryption by the key she shares with Trent, and this message is received by Bob.

- Generating a second message comprising second values for a second random number and information identifying said access point and said wireless client and a second message authentication code of said information in said second message signed using a second signing key.
  - Where the second message is generated by Bob, the second random number is Nonce B, information identifying the access point is Bob's Name, information identifying the wireless client is Alice's name, the second message authentication code is an index number, and the message is signed or encrypted using another key, the one Bob shares with Trent.
- Sending said first values and said second values to an access point server, wherein said access point server generates a session key using said first and second values and third values provided by said access point server.
  - Where the message generated by Bob and Alice, are eventually both sent to Trent, the Access point server, where the first value is the random number of Alice, the second value is the random number of Bob. The session key is the session key generated by Trent.

Menezes et al. however fails to explicitly disclose using the first and second Nonce and generating a third value to be used in the generation of the session key. Menezes et al. also fails to explicitly disclose the hardware embodiment where Alice is a Wireless client, Bob is the Access point, and Trent is the Access Point server.

Key generation may employ any number of values. Schneier (p. 175, "X9.17 key generation") for example discloses X9.17 key generation which uses three different seeds for the generation of a key. Schneier (p. 175, "X9.17 key generation", Applied Cryptography) further discloses that this method does not generate easy to remember keys, making it suitable for session keys.

Lincke et al. (Figure 4) discloses the use of a wireless client communicating with an access point, which then in turn communicates with a server. This setup appears to be common in wireless technology as a standard wireless topology. Additionally, Menezes et al. describes Alice, Bob, and Trent, as parties A, B, and T, suggesting that any digital processing device may be used to implement them and that only their respective interactions are important.

It would have been obvious to one of ordinary skill in the art to implement Alice, Bob, and Trent as the wireless client, wireless access point, and server, and to use they X9.17 key generation process to generate keys appropriate for use as session keys and to provide the benefits of the Otway-Rees algorithm in a wireless context.

However, neither Menezes et al, Lincke et al., or Schneier "Applied Cryptography" discloses an embodiment of Otway Rees encryption in which the first and second values are combined together as Applicant has amended. No art can be found which discloses this combination in the context of an Otway Rees protocol nor motivation to combine uncovered. In contrast, it is simply presumed by Otway Rees protocol that both values will be accessible to a server for use in computation by the session key.

For this reason, claim 1 is held to be allowable.

Additionally, the Applicant has also recited that the processing is "shared by said access point and said access point server" page 10 of Applicant's arguments in the communication of 11/1/05 reveals that Applicant considers the processing to be shared by generating the message that includes the combined first and second values, and by the manipulations that result as a consequence of using a third value. Neither Menezes et al, Lincke et al., or Schneier "Applied Cryptography" explicitly discloses this shared processing either, and claim 1 is further allowable for these reasons.

Independent claims 9 and 17 are substantially similar to claim 1 and are allowable for the same reasons.

All other claims dependent claims depending from claims 1, 9, or 17 and are allowable because their independent claims are allowable.

Conclusion

4. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (571)272-3838.

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist	Telephone: 571-272-2100	Fax: 703-872-9306
Customer Service Representative	Telephone: 571-272-2100	Fax: 703-872-9306

TMH

January 19th, 2006

E. Moise
EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER